Audit Report

U.S. SPECIAL OPERATIONS COMMAND YEAR 2000 ISSUES

Report No. 98-129

MAY 8, 1998

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: U.S. Special Operations Command Year 2000 Issues

B. DATE Report Downloaded From the Internet: 09/21/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #):

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/21/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, Home Page at: WWW.DODIG.OSD.MIL.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

SOCOM	U.S. Special Operations Command
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

May 8, 1998

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. SPECIAL OPERATIONS COMMAND
DIRECTOR, JOINT STAFF

SUBJECT: Audit Report on U.S. Special Operations Command Year 2000 Issues (Report No. 98-129)

We are providing this audit report for information and use. We considered comments on a draft of this report in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Mary Lu Ugone, at (703) 604-9049 (DSN 664-9049); or Ms. Dianna J. Pearson, at (703) 604-9063 (DSN 664-9063). See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Robert J Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-129 **May 8, 1998**
(Project No. 8AS-0006.00)

U.S. Special Operations Command Year 2000 Issues

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge.

Information technology systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve electronic storage and reduce operating costs. With the two-digit format, however, the year 2000 is indistinguishable from 1900. As a result of the ambiguity, computers and associated systems and application programs that use dates to calculate, compare, and sort could generate incorrect results when working with years after 1999.

Audit Objectives. The overall audit objective was to evaluate the status of the U. S. Special Operations Command's progress in resolving the year 2000 computing issue. Our audit focused on the following year 2000 issues: leadership support and awareness, management and resolution strategy, system assessments, prioritization, system interfaces, testing, risk analysis and contingency planning, and support received from responsible Service executive agents. We did not review the management control program related to the overall audit objective because DoD recognizes the year 2000 issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Audit Results. The U.S. Special Operations Command has recognized the importance of the year 2000 issue and has taken numerous positive actions in addressing the year 2000 problem. Additionally, the U.S. Special Operations Command advocates using existing planned exercises to test year 2000 scenarios in an operational environment. We strongly agree.

The progress that the U.S. Special Operations Command made in resolving the year 2000 computing issue is not complete. Unless the U.S. Special Operations Command makes further progress, it faces a high risk that year-2000-related disruptions will impair its mission capabilities. See Part I for details of the audit results.

Summary of Recommendations. We recommend that the Commander in Chief, U.S. Special Operations Command, review changes to the DoD Year 2000 Management Plan and take appropriate action based on those changes; continue to identify mission-critical systems that the U.S. Special Operations Command manages; continue to identify interfaces and prepare written interface agreements for mission-critical systems that the U.S. Special Operations Command manages; continue to identify mission-critical supporting systems that Services or other organizations manage; refine cost estimates for each individual system to determine amounts needed for fund allocation; develop contingency plans for mission-critical systems in accordance with the U.S. Special Operations Command Year 2000 Management Plan; determine systems as year 2000 compliant only after testing and completing compliance checklists; and use selected command and joint exercises to test year 2000 scenarios in an operational environment. We recommend that the Director, Joint Staff, assist the unified commands in obtaining year 2000 information on mission-critical supporting systems that Services or other organizations manage; assist the unified commands in testing systems and applications common to the unified commands; and use selected joint exercises to test year 2000 scenarios in an operational environment.

Management Comments. The U.S. Special Operations Command concurred with all of the recommendations, stating progress made and future intentions for each recommendation. The Joint Staff concurred with the recommendations, stating actions that it is taking to address the issues. See Part I for a summary of management comments and Part III for the complete text of the comments.

Table of Contents

Part I - Audit Results

Audit Background

The year 2000 (Y2K) problem is the term most often used to describe the potential failure of information technology systems to process or perform date-related functions before, on, or after the turn of the century. The Y2K problem is rooted in the way that automated information systems record and compute dates. For the past several decades, systems have typically used two digits to represent the year, such as "98" representing 1998, to conserve on electronic data storage and reduce operating costs. With the two-digit format, however, the Y2K is indistinguishable from 1900. As a result of the ambiguity, computers and associated system and application programs that use dates to calculate, compare, or sort could generate incorrect results when working with years following 1999. Calculation of Y2K dates is further complicated because the year 2000 is a leap year, the first century leap year since 1600. The computer systems and applications must recognize February 29, 2000, as a valid date.

Because of the potential failure of computers to run or function throughout the Government, the President issued an Executive Order, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the Y2K problem and that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency. In addition, the General Accounting Office has designated resolution of the Y2K problem as a high-risk area, and DoD recognized the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

DoD Y2K Management Strategy. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" (DoD Management Plan) in April 1997. The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, fixing, or retiring systems, and monitoring progress. The DoD Management Plan states that the DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem. Also, the DoD Management Plan makes the DoD Components responsible for the five-phase Y2K management process. The DoD Management Plan includes a description of the five-phase Y2K management process.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is in the process of issuing an updated DoD Management Plan, which further accelerates the target completion dates for the Renovation, Validation, and Implementation phases, resulting in a completion date of December 1998.

In a memorandum for the heads of executive departments and agencies dated January 20, 1998, the Office of Management and Budget established a new target date of March 1999 for implementing all corrective actions to all systems. The new target completion dates are September 1998 for the Renovation phase and January 1999 for the Validation phase.

The Joint Chiefs of Staff. The Chairman of the Joint Chiefs of Staff is the principal military advisor to the President, the Secretary of Defense, and the National Security Council. The Joint Chiefs of Staff have no executive authority to command the combatant forces. The Secretaries of the Military Departments assign all forces under their jurisdiction to the unified commands to perform missions assigned to those commands.

The Joint Staff. The Joint Staff assists the Chairman of the Joint Chiefs of Staff with unified strategic direction of the combatant forces, unified operation of the combatant commands, and integration into an efficient team of land, naval, and air forces. The Joint Staff Director, Command, Control, Communications, and Computer Systems (J6), has been designated by the Chairman of the Joint Chiefs of Staff to oversee the unified commands' and Joint Staff's implementation of the DoD Y2K Management Plan.

Year 2000 Action Plan. The Joint Staff Year 2000 Action Plan, March 1998, provides the unified commands and Joint Staff directorates with the corporate strategy and management approach for addressing the Y2K problem. The Joint Staff Action Plan uses the accelerated target completion dates for the Renovation, Validation, and Implementation phases. The Joint Staff Year 2000 Action Plan states that the unified commands should target December 31, 1998, for completion of all Y2K efforts.

U.S. Special Operations Command. The U.S. Special Operations Command (SOCOM) is one of nine unified commands in the U.S. military's combatant command structure. The SOCOM was activated on April 16, 1987, as a result of the Cohen-Nunn amendment to the National Defense Authorization Act for FY 1987. The overall mission of SOCOM is to prepare special operations forces to successfully conduct worldwide special operations, civil affairs, and psychological operations in peace and war in support of the regional combatant commanders, American ambassadors and their country teams, and other Government agencies.

Congress created SOCOM to correct serious deficiencies in the United States' ability to conduct special operations and engage in low-intensity conflict activities. The SOCOM was assigned many Service-like responsibilities, including training, ensuring combat readiness, monitoring personnel promotions and assignments, and developing and acquiring special operations forces-peculiar equipment. The SOCOM was also given responsibility for managing a separate major force program to ensure that the special operations forces program has visibility at the DoD and congressional levels. The four component commands of SOCOM are the Army Special Operations Command, the Naval Special Warfare Command, the Air Force Special Operations Command, and the Joint Special Operations Command. Additionally, the special operations commands and personnel from civil affairs and psychological operations provide special operations forces to the geographic unified commands.

Audit Objectives

The overall audit objective was to evaluate the status of the progress of SOCOM in resolving its Y2K computing issue. Our audit focused on the following Y2K issues: leadership support and awareness, management and resolution strategy, system assessments, prioritization, system interfaces, testing, risk analysis and contingency planning, and support received from responsible Service executive agents. We did not review the management control program related to the overall audit objective because DoD recognizes the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance. See Appendix A for a discussion of the audit scope and methodology and Appendix B for a summary of prior audit coverage.

Status of the U.S. Special Operations Command Year 2000 Program

The SOCOM has recognized the importance of the Y2K issue and has taken many positive actions to address the Y2K problem. Additionally, SOCOM advocates using selected command and joint exercises to test Y2K scenarios in an operational environment. The progress that SOCOM made in resolving the Y2K computing issue is not complete because SOCOM did not fully address several critical issues. To ensure that its mission-critical systems will successfully operate at the Y2K and beyond, SOCOM, including its component commands and functional directorates, must further do the following to address critical issues:

- review changes to the DoD Y2K Management Plan and take appropriate action based on the changes;
- continue to identify mission-critical systems that SOCOM manages;
- continue to identify interfaces and prepare written interface agreements for mission-critical systems that SOCOM manages;
- continue to identify mission-critical supporting systems that Services or other organizations manage;
- refine cost estimates for each individual system to determine the amounts needed for fund allocation;
- develop contingency plans for mission-critical systems in accordance with the SOCOM Y2K Management Plan;
- determine systems as Y2K compliant only after testing the systems and completing compliance checklists; and
- use selected command and joint exercises to test Y2K scenarios in an operational environment.

Designating Y2K as a Commander's special interest item in selected exercises to test Y2K scenarios may assist SOCOM in making further progress in identifying and resolving Y2K problems. Unless SOCOM makes further progress, it faces a high risk that Y2K-related disruptions will impair its mission capabilities.

Actions Taken to Address the Year 2000 Problem

The SOCOM has recognized the importance of the Y2K issue and has taken many positive actions to address the Y2K problem. The SOCOM has established a Y2K program management structure that provides management awareness and involvement in developing and executing the SOCOM Y2K strategy. Additionally, SOCOM advocates using selected command and joint exercises to test Y2K scenarios in an operational environment. We strongly agree.

Specific Actions. The SOCOM has taken the following actions as part of its efforts to address the Y2K problem:

- developed a SOCOM Y2K Management Plan that establishes strategies, policies, and procedures that SOCOM will follow to identify and resolve Y2K issues;

- established the SOCOM Y2K Steering Group and the SOCOM Acquisition Executive Integrated Project Team to assist in Y2K efforts;

- reinforced the importance of Y2K efforts at top levels of management; and

- initiated contact and established a working relationship with the Joint Interoperability Test Command on testing issues.

The DoD Chief Information Officer has updated the DoD Y2K Management Plan and has released a new version in draft. The SOCOM needs to review changes to the DoD Y2K Management Plan and take appropriate action based on those changes.

Y2K Program Management. The Director of Command, Control, Communications, Computers, and Information Systems, who also serves as the SOCOM Chief Information Officer, has principal staff oversight for the Y2K project. The SOCOM has the Y2K Steering Group and the SOCOM Acquisition Executive Integrated Project Team to assist in Y2K efforts. The SOCOM Y2K Steering Group assists the Directorate of Command, Control, Communications, Computers, and Information Systems in the development and execution of the Y2K strategy of SOCOM. The Y2K Steering Group's focus is on developing an affordable and executable strategy. The core membership consists of representatives from each of the functional directorates, as well as the Command Engineer and the SOCOM Acquisition Executive. In addition, the SOCOM Acquisition Executive organized the Y2K Integrated Project Team to manage and provide oversight to the Y2K-vulnerable systems that the SOCOM Acquisition Executive manages.

Identification of Systems and Interfaces

The SOCOM component commands and functional directorates need to be more engaged in the identification of mission-critical systems interfaces, especially the mission-critical supporting systems that Services or other organizations manage. Managed systems are those for which SOCOM has program management responsibility. Supporting systems are those that Services or other organizations manage. As of November 1997, SOCOM identified 35 SOCOM-managed systems and 82 supporting systems. The SOCOM determined that 12 of the 35 SOCOM-managed systems are mission critical, but it has not identified any of the 82 supporting systems as mission critical. Based on management comments, SOCOM identified 37 SOCOM-managed mission-critical systems, as of February 23, 1998, and has identified 68 mission-critical supporting systems, as of April 10, 1998. Table B-1 in Appendix B provides the number and type of SOCOM systems.

Systems Inventory. The SOCOM developed its original list of systems in December 1996 from a budget database. The SOCOM used the budget database because the information received from the SOCOM functional directorates and component commands included a small number of systems and a large number of desktop computers, and therefore the information was not sufficient. In addition, the SOCOM Acquisition Executive used a payments database to help identify SOCOM systems. The SOCOM Acquisition Executive identified the systems in the payments database and determined who was responsible for resolving Y2K issues.

The SOCOM then merged the budget database and the payments database and performed further assessments on the systems to develop a more accurate and complete list of systems. However, SOCOM is continually updating the system inventory list. For example, in its initial Y2K assessment, SOCOM identified and reported 85 systems as reportable. However, for the first quarter FY 1998 quarterly report, SOCOM determined that 26 systems were SOCOM Y2K reportable systems and recategorized the other 59 systems as supporting systems. In addition to recategorizing 59 systems from SOCOM-managed systems to supporting systems, the list of supporting systems is evolving. For example, SOCOM has not confirmed an executive agent for 11 of the 82 supporting systems. Also, 5 of those 11 systems show 2 responsible organizations. The SOCOM needs more assistance from the Joint Staff to obtain Y2K information for supporting systems that Services or other organizations manage.

Mission-Critical Systems. The SOCOM, through the SOCOM Y2K Steering Group, has identified 12 of the 35 SOCOM-managed systems as mission critical, as of November 1997. However, SOCOM has not identified any of the 82 supporting systems as mission critical. We reviewed the Services' and the Defense Information Systems Agency's mission-critical systems lists. As of November 1997, the lists identify only 9 of the 54 supporting systems belonging to the Services and Defense Information Systems Agency as mission critical. The SOCOM, with the help of its component commands and the functional directorates, needs to identify mission-critical supporting systems because the appropriate executive agents need to be aware of the systems that are critical to the SOCOM mission. After SOCOM has identified the mission-critical supporting systems, the Joint Staff should assist SOCOM and the other unified commands in obtaining Y2K information on mission-critical supporting systems that Services or other organizations manage.

Based on management comments, SOCOM identified 37 SOCOM-managed mission-critical systems, as of February 23, 1998, and has identified 68 mission-critical supporting systems, as of April 10, 1998.

Interfaces. The SOCOM has not completed identifying system interfaces and preparing written interface agreements. The DoD Y2K Management Plan states that interfaces involve sending and receiving data among Services, Defense agencies, or both, or external DoD vendors. Interfaces are critical to the Y2K effort because they have the potential to introduce or propagate errors, or both, from one DoD Component to another. The systems of SOCOM interface with or connect to many computer systems belonging to the Services, DoD Components, and other organizations. In addition to known interfaces, SOCOM may interface with systems of allied, coalition, and other Federal agencies. Because those systems are also vulnerable to Y2K problems, they can also introduce or propagate errors, or both, into SOCOM systems. Timely and complete information on all system interfaces that may be affected by Y2K changes is critical to the success of the Y2K compliance program of SOCOM.

Written Interface Agreements

After SOCOM identifies interfaces, it should communicate through interface agreements its interface plans to interface partners so that they are aware of SOCOM plans and any possible conflicts. The sample Y2K compliance checklist in the DoD Y2K Management Plan states that DoD Components and each interface partner should negotiate an agreement dealing with Y2K issues. The DoD Components and their interface partners should discuss and verify that they have implemented consistent Y2K corrections for data passed between the systems. The SOCOM needs to prepare written interface agreements to reduce the risk of discovering too late in the Y2K effort that an interfacing system will not be able to accommodate the agency's own Y2K changes.

Based on management comments, as of March 1998, SOCOM has identified 141 interfaces between SOCOM-managed systems and supporting systems that Services or other organizations manage. The SOCOM has identified August 3, 1998, as the target completion date for all interface memorandums of agreement.

Cost Estimates

The SOCOM has made initial cost estimates based on available information; however, SOCOM has not refined the cost estimates for each individual system. Many factors influence cost estimates, including building the test environment, buying tools and services, adding hardware, and upgrading operating systems software and commercial products. In addition, unidentified testing costs may increase the overall Y2K estimated cost. The SOCOM can develop cost estimates from the checklist in the DoD Y2K Management Plan or by any other accurate means; however, the DoD Y2K Management Plan states that DoD Components must identify the methodology used to develop the cost estimates. As of November 1997, SOCOM has spent approximately $850,000 on Y2K costs, with a total estimated Y2K cost of $5.8 million. The SOCOM is aggressively seeking ways to reallocate funds to cover the $5.8 million. Based on management comments, as of April 10, 1998, SOCOM identified $11 million as required to fix the Y2K non-compliant systems.

Contingency Plans

The SOCOM has not developed contingency plans for each system. The DoD Y2K Management Plan states that DoD Components should develop realistic contingency plans, including the development and activation of manual or contract procedures to ensure the continuity of core processes. The SOCOM is scheduled to start developing contingency plans in March 1998 and to complete them by August 1998. Contingency plans may already exist for some mission-critical systems. Those that may have automation as the backup need to assess the backup for Y2K issues.

Testing and Compliance Checklists

The SOCOM reports that 17 of 35 managed systems are Y2K compliant, and 5 of 12 mission-critical managed systems are Y2K compliant. However, SOCOM made that determination without testing, without identifying all interfaces for those systems, and without completing compliance checklists. The systems that SOCOM initially assessed as Y2K compliant are placed in the "validation" phase. The SOCOM should not report the systems as Y2K compliant until the systems have been tested and certified.

Testing. The DoD Y2K Management Plan states that DoD Components need an extensive period of time to adequately validate and test converted or replaced systems for Y2K compliance. DoD Components must not only test Y2K compliance of individual applications, but must also test the complex interactions between scores of converted or replaced computer platforms, operating systems, utilities, applications, databases, and interfaces. All converted or replaced system components introduced during the "renovation" phase must be thoroughly validated and tested to uncover errors, validate Y2K compliance, and verify operational readiness. The Joint Staff should assist the unified commands in testing systems and applications common to the unified commands.

As of November 1997, the Joint Interoperability Test Command is either renovating or testing seven systems and devices, four of which are mission critical, that SOCOM manages. However, SOCOM has not identified all the system interfaces that require testing. The Joint Interoperability Test Command provides general assistance in Y2K resolution that includes test planning, test case development, and solution recommendations. The SOCOM provides funding if SOCOM requires contractor support or the use of the Defense megacenters. The SOCOM also provides funding for any travel required by Government or contractor personnel. In addition, the Joint Interoperability Test Command can provide specific assistance in support of a system to include analysis of hardware platforms and software application packages, development and execution of a Y2K test plan, recommendations to resolve Y2K impacts, and implementation of resolution recommendations.

Compliance Checklists. Although SOCOM has an aggressive compliance plan, it has not followed the plan for all systems. The DoD Y2K Management Plan states that DoD Components should develop and document test and compliance plans and schedules for each converted or replaced application or system component. The DoD Y2K Management Plan provides a Y2K-compliance checklist to aid system managers in ensuring that their systems are compliant for the Y2K. The compliance checklist provided in the DoD Y2K Management Plan lists items that should be included in a DoD Component's Y2K testing and compliance process. The SOCOM developed a Y2K-compliance certification plan that provides the instructions for determining compliance of information technology, software, and systems that have a Y2K problem. The SOCOM compliance certification plan also provides the steps necessary to ascertain whether information technology systems have been correctly modified to ensure a non-impact transition from the twentieth century to the twenty-first century. The SOCOM compliance certification plan states that those systems deemed properly modified will be certified as Y2K compliant. In addition, the SOCOM compliance certification plan requires certifications from the test manager, system manager, and system customer for each compliance checklist. The SOCOM is developing an applications test bed to provide Y2K testing for in-house-generated database applications.

Use of Selected Command and Joint Exercises to Test Y2K Scenarios

The SOCOM advocates using selected exercises to test Y2K scenarios in an operational environment. We strongly agree. Unified command exercises test operational plans, validate force apportionment, support political and military relationships and objectives, and foster regional engagements of unified commanders. Joint exercises include joint training events based on approved joint doctrine that prepares joint forces or staffs to respond to operational requirements established by the combatant commanders to accomplish their assigned missions. Mission focus is critical to the effectiveness and efficiency of joint training exercises. The goals of joint training are to prepare for war, prepare for military operations other than war, prepare for multinational operations, and integrate the interagency process. The joint exercises focus on plans, policies, procedures, and training required to ensure that senior leaders can effectively direct and integrate U.S. and coalition military forces during war. Common operational joint tasks are activities conducted by or for multiple supported commands under similar conditions and to a common joint standard.

The common tasks are selected by multiple combatant commands through the mission analysis process, and they describe a list of core joint competencies that are fundamental to joint operations. The common joint tasks include the following:

- conducting operational movement and maneuvers,
- developing operational intelligence,
- employing operational firepower,
- providing operational support,
- exercising operational command and control, and
- providing operational protection.

Selected command and joint exercises could be used to measure the extent of potential Y2K problems that face the warfighter and allow time to correct critical problems. Because of time constraints posed by Y2K issues, using selected command and joint exercises to test Y2K scenarios may assist SOCOM in making further progress to identify and resolve Y2K problems.

Conclusion

Although SOCOM has made initial progress, it must continue to address several critical issues. SOCOM has recognized the importance of solving Y2K problems in its systems to reduce the risk of failure with its own Y2K effort, but SOCOM must take every possible measure to ensure that it is well-positioned to deal with unexpected problems and delays. Y2K testing would be a timely Commander's special interest item for 1998 in the joint exercise scenario development. The nation's special operations forces provide the National Command Authorities with a highly trained, rapidly deployable joint force that is capable of conducting special operations anywhere in the world. Unless SOCOM makes further progress, it faces a high risk that its mission capabilities will be impaired because of Y2K-related disruptions. Copies of this report are being provided to all unified commands to facilitate self reviews of Y2K efforts.

Recommendations and Management Comments

1. We recommend that the Commander in Chief, U.S. Special Operations Command:

a. Review changes to the "DoD Year 2000 Management Plan," and take appropriate action based on those changes.

b. Continue to identify mission-critical systems that the U.S. Special Operations Command manages.

c. Continue to identify interfaces and prepare written interface agreements for mission-critical systems that the U.S. Special Operations Command manages.

d. Continue to identify mission-critical supporting systems that Services or other organizations manage.

e. Refine cost estimates for each individual system to determine amounts needed for fund allocation.

f. Develop contingency plans for mission-critical systems in accordance with the U.S. Special Operations Command Year 2000 Management Plan.

g. Determine systems as year 2000 compliant only after testing the systems and completing compliance checklists.

h. Use selected command and joint exercises to test year 2000 scenarios in an operational environment.

Management Comments. The SOCOM concurred with all of the recommendations, stating progress made and future intentions for each recommendation.

2. We recommend that the Director, Joint Staff:

a. Assist the unified commands in obtaining year 2000 information on mission-critical supporting systems that Services or other organizations manage.

b. Assist the unified commands in testing systems and applications that are common to the unified commands.

c. Use selected joint exercises to test year 2000 scenarios in an operational environment.

Management Comments. The Joint Staff concurred with the recommendations, stating actions that it is taking to address the issues.

Part II - Additional Information

Appendix A. Audit Process

Scope

This is one of a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the Y2K issue, see the Y2K webpage on IGnet at http://www.ignet.gov.

We reviewed and evaluated the status of the progress of SOCOM in resolving the Y2K computing issue. We evaluated the Y2K efforts of SOCOM, compared with those efforts described in the DoD Y2K Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in April 1997. We obtained documentation including the SOCOM Draft Y2K Management Plan, the SOCOM Y2K Compliance Certification Plan, and systems inventory database information. We used the information to assess efforts related to the multiple phases of managing the Y2K problem.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from October 1997 through January 1998 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1997 Annual Statement of Assurance.

Prior Audit Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil.

Appendix B. Reporting, Schedule, and Area of Concern

External and Internal Reporting

Y2K Reporting Requirements. DoD Components* are required to submit Y2K quarterly reports to the DoD Chief Information Officer to satisfy both DoD and Office of Management and Budget reporting requirements.

DoD Reporting Requirements. On March 12, 1997, the DoD Chief Information Officer issued the memorandum, "Year 2000 Refined Reporting Requirements for DoD," which established minimum quarterly reporting requirements for Y2K assessment and progress for 23 DoD Components. The information is intended to show the status of DoD Y2K efforts and is being used by the DoD Chief Information Officer to perform oversight for DoD Y2K efforts and to fulfill Office of Management and Budget reporting requirements at the DoD level.

Office of Management and Budget Reporting Requirements. On May 7, 1997, the Office of Management and Budget issued the "Memorandum on Computer Difficulties Due to the Year 2000 -- Progress Reports." The purpose of the memorandum is to provide Y2K progress reports to Congress and the public. Each agency is required to report on mission-critical systems, including information on the number of systems that are Y2K compliant, are being replaced, are being repaired, and are being retired.

SOCOM External Reporting Process. The Joint Staff and the nine unified commands comprise one of the 23 DoD Components identified for Y2K quarterly reporting. The SOCOM sends its quarterly report information to the Joint Staff. The Joint Staff then submits the SOCOM information, along with other unified command information and the Headquarters, Joint Staff, information to the DoD Chief Information Officer. The DoD Chief Information Officer uses the information in the Joint Staff quarterly report for the overall DoD Y2K report that it sends to the Office of Management and Budget.

*The 23 DoD Components include all Defense agencies and the Services. Some of the smaller Defense agencies are consolidated into 1 of the 23 DoD Components.

SOCOM Internal Reporting Process. The SOCOM has instituted an internal Y2K reporting structure to provide an overview of SOCOM system progress through various phases of the Y2K management process. The information is used to assist the SOCOM Y2K Steering Group in managing the overall Y2K effort. Table B-1 shows the number of systems and reporting categories for SOCOM.

Table B-1. SOCOM Y2K Systems Status
(as of November 12, 1997)[1,2]

Systems Type	Number
SOCOM-managed	
Managed systems	35[1]
Internal applications	43
Devices	11
Not SOCOM-managed	
Supporting systems	82[2]
Supporting devices	1
COTS/GOTS[3] hardware	334
COTS/GOTS software	154

[1] The SOCOM originally identified 12 SOCOM-managed systems as mission critical. Based on management comments, as of February 23, 1998, SOCOM identified 37 SOCOM-managed systems as mission critical. The SOCOM did not identify the total number of managed systems in their comments.

[2] The SOCOM originally identified 0 supporting systems as mission critical. Based on management comments, as of April 10, 1998, SOCOM identified 68 mission-critical supporting systems. The SOCOM did not identify the total number of supporting systems in their comments.

[3] Commercial off-the-shelf, Government off-the-shelf.

Source: SOCOM.

Schedule

The overall SOCOM Y2K effort is organized into five specific phases with principal milestones established for each phase. To further facilitate project management and coordination, SOCOM has established additional target dates within each phase. The SOCOM Management Plan states that the dates are critical and immovable, and therefore compliance timelines must be accomplished in accordance with the Y2K project schedule. Table B-2 shows the summary of the phases and milestones.

Table B-2. SOCOM Y2K Program Phases and Milestones

	Milestones	
Phase	Start	Finish
1. Awareness - informing	July 1996	Ongoing
2. Assessment - Y2K compliance determination	March 1997	October 1997
2.5. Damage control contingency planning	March 1998	August 1998
3. Renovation - fix problems		
3.1. Determine cost	June 1997	November 1997
3.2. Determine schedule	November 1997	January 1998
3.3. Fix the problem	January 1998	August 1998
4. Validation - testing solutions and Y2K compliance	January 1998	December 1998
5. Implementation - fielding compliant systems	January 1998	July 1999

SOCOM Area of Concern

Although SOCOM is aggressively seeking ways to reallocate funds to cover the $5.8 million estimated cost of the Y2K program, DoD funding for Y2K would help the overall Y2K program to succeed. Based on management comments, as of April 10, 1998, SOCOM identified $11 million as required to fix the Y2K non-compliant systems.

Appendix C. Report Distribution

Office of the Secretary of Defense

Deputy Secretary of Defense
Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Acquisition Reform)
  Deputy Under Secretary of Defense (Logistics)
  Director, Defense Procurement
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  DoD Year 2000 Project Officer
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Air Force

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Ballistic Missile Defense Organization
  Chief Information Officer, Ballistic Missile Defense Organization
Director, Defense Advanced Research Projects Agency
  Chief Information Officer, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
  Chief Information Officer, Defense Commissary Agency
Director, Defense Contract Audit Agency
  Chief Information Officer, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
  Chief Information Officer, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
Director, Defense Legal Services Agency
  Chief Information Officer, Defense Legal Services Agency
Director, Defense Logistics Agency
  Chief Information Officer, Defense Logistics Agency
Director, Defense Security Assistance Agency
  Chief Information Officer, Defense Security Assistance Agency
Director, Defense Security Service
  Chief Information Officer, Defense Security Service
Director, Defense Special Weapons Agency
  Chief Information Officer, Defense Special Weapons Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, On-Site Inspection Agency
  Chief Information Officer, On-Site Inspection Agency
Director, Washington Headquarters Services
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency

Non-Defense Federal Organizations and Individuals

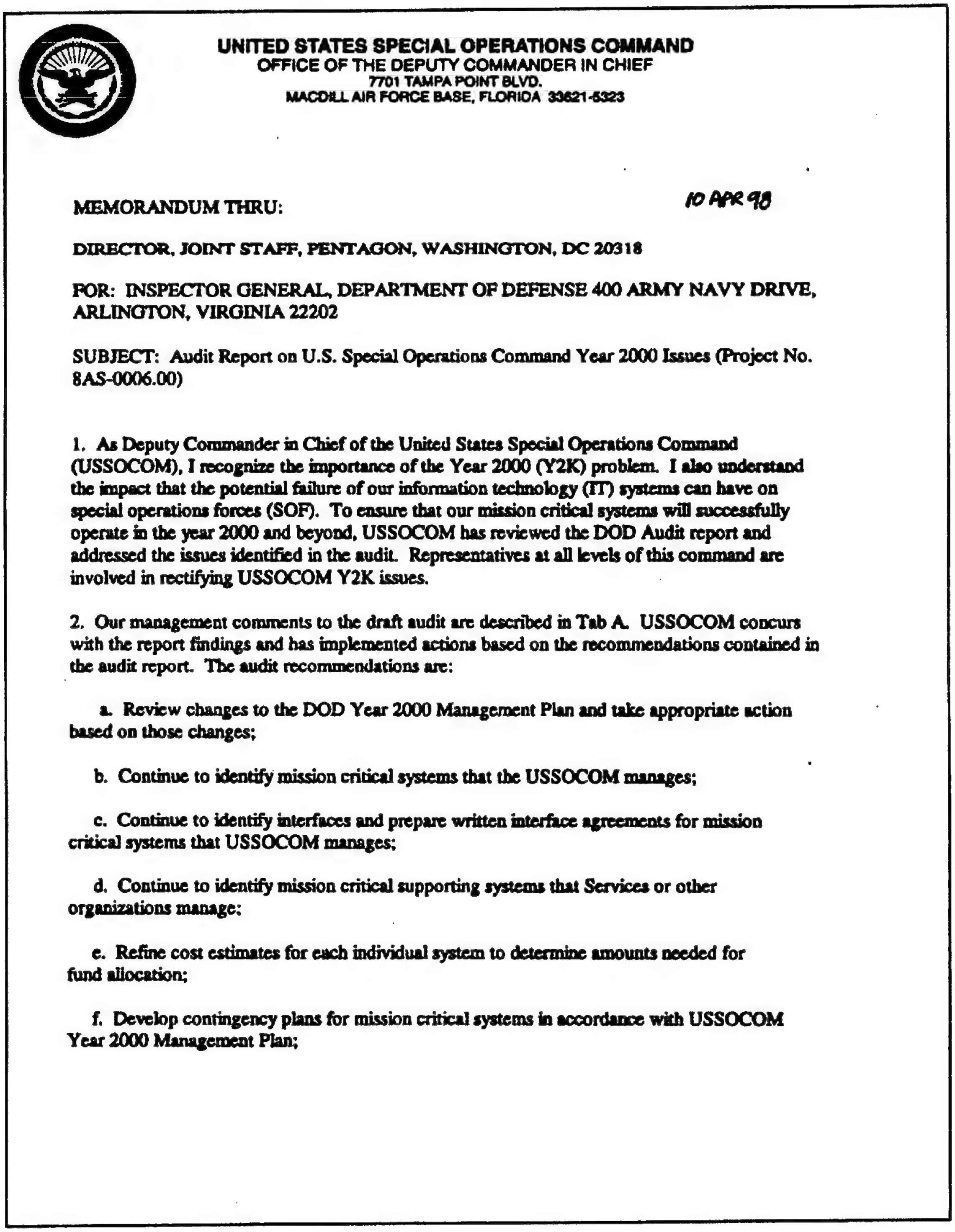
Chief Information Officer, General Services Administration
Office of Management and Budget
  Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division, General Accounting Office
Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Special Committee on the Year 2000 Technology Problem
Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Governmental Reform and Oversight
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security

Part III - Management Comments

U.S. Special Operations Command Comments



UNITED STATES SPECIAL OPERATIONS COMMAND
OFFICE OF THE DEPUTY COMMANDER IN CHIEF
7701 TAMPA POINT BLVD.
MACDILL AIR FORCE BASE, FLORIDA 33621-5323

MEMORANDUM THRU: 10 APR 98

DIRECTOR, JOINT STAFF, PENTAGON, WASHINGTON, DC 20318

FOR: INSPECTOR GENERAL, DEPARTMENT OF DEFENSE 400 ARMY NAVY DRIVE, ARLINGTON, VIRGINIA 22202

SUBJECT: Audit Report on U.S. Special Operations Command Year 2000 Issues (Project No. 8AS-0006.00)

1. As Deputy Commander in Chief of the United States Special Operations Command (USSOCOM), I recognize the importance of the Year 2000 (Y2K) problem. I also understand the impact that the potential failure of our information technology (IT) systems can have on special operations forces (SOF). To ensure that our mission critical systems will successfully operate in the year 2000 and beyond, USSOCOM has reviewed the DOD Audit report and addressed the issues identified in the audit. Representatives at all levels of this command are involved in rectifying USSOCOM Y2K issues.

2. Our management comments to the draft audit are described in Tab A. USSOCOM concurs with the report findings and has implemented actions based on the recommendations contained in the audit report. The audit recommendations are:

a. Review changes to the DOD Year 2000 Management Plan and take appropriate action based on those changes;

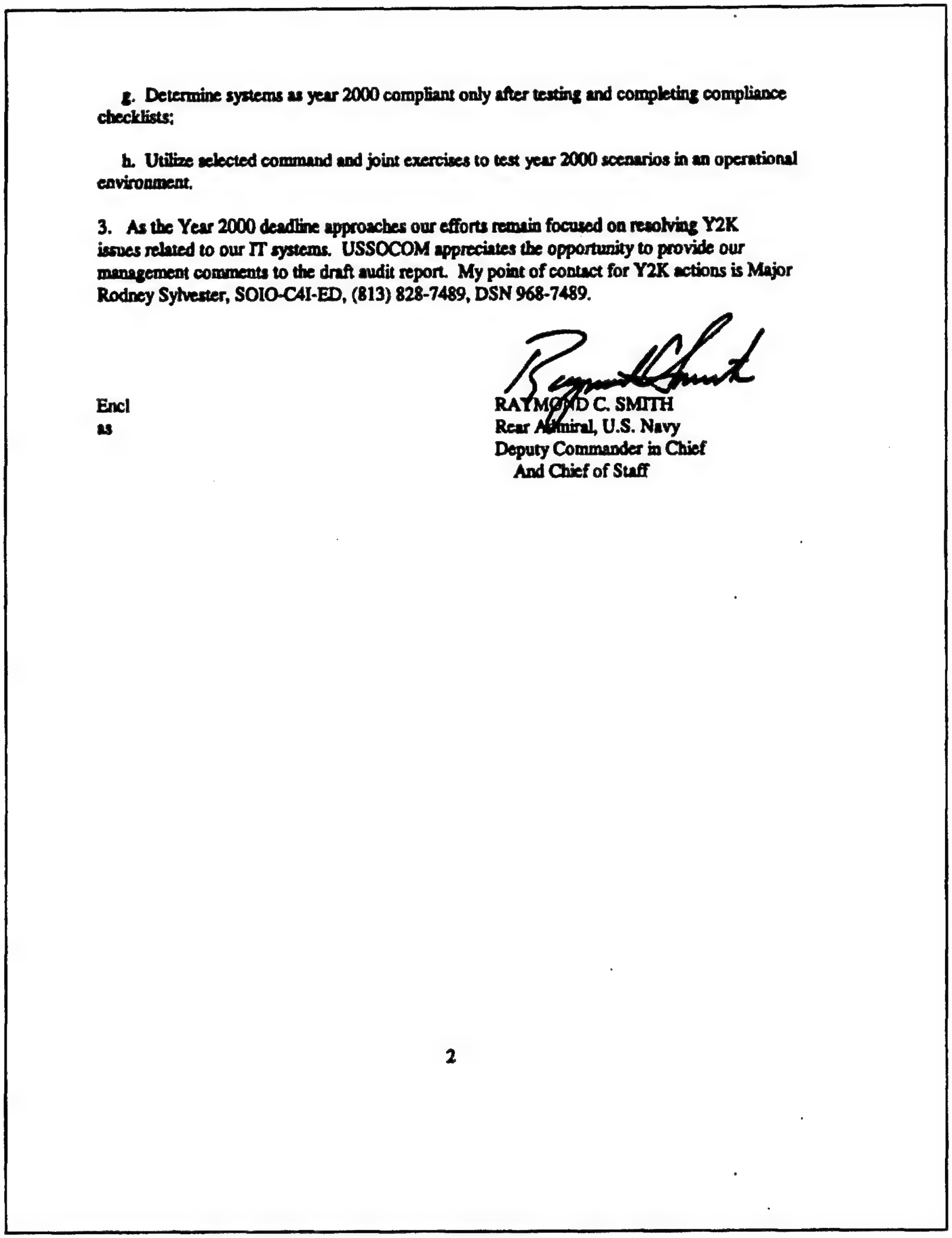
b. Continue to identify mission critical systems that the USSOCOM manages;

c. Continue to identify interfaces and prepare written interface agreements for mission critical systems that USSOCOM manages;

d. Continue to identify mission critical supporting systems that Services or other organizations manage;

e. Refine cost estimates for each individual system to determine amounts needed for fund allocation;

f. Develop contingency plans for mission critical systems in accordance with USSOCOM Year 2000 Management Plan;



g. Determine systems as year 2000 compliant only after testing and completing compliance checklists;

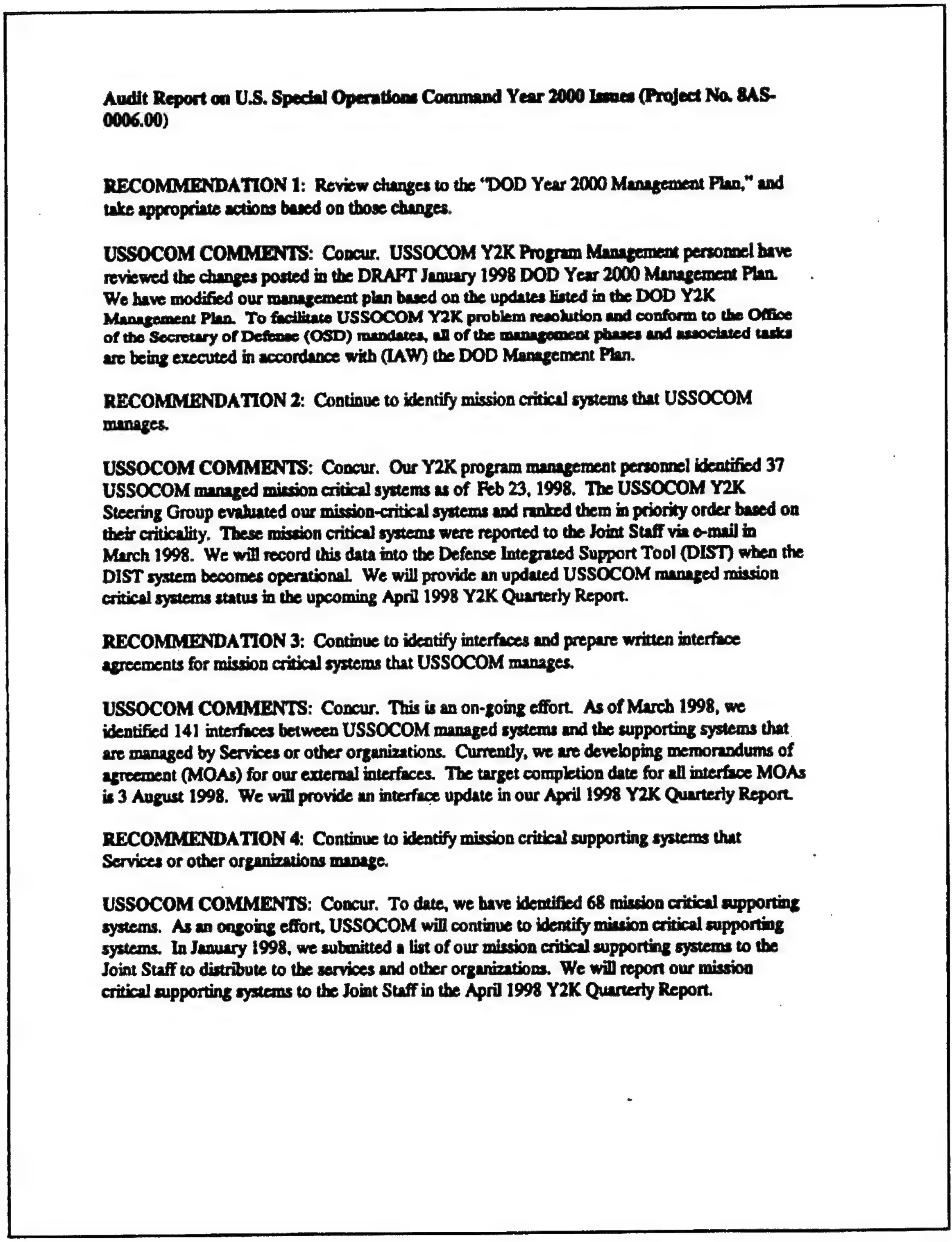
h. Utilize selected command and joint exercises to test year 2000 scenarios in an operational environment.

3. As the Year 2000 deadline approaches our efforts remain focused on resolving Y2K issues related to our IT systems. USSOCOM appreciates the opportunity to provide our management comments to the draft audit report. My point of contact for Y2K actions is Major Rodney Sylvester, SOIO-C4I-ED, (813) 828-7489, DSN 968-7489.

Encl
as

RAYMOND C. SMITH
Rear Admiral, U.S. Navy
Deputy Commander in Chief
And Chief of Staff

U.S. Special Operations Command Comments



Audit Report on U.S. Special Operations Command Year 2000 Issues (Project No. 8AS-0006.00)

RECOMMENDATION 1: Review changes to the "DOD Year 2000 Management Plan," and take appropriate actions based on those changes.

USSOCOM COMMENTS: Concur. USSOCOM Y2K Program Management personnel have reviewed the changes posted in the DRAFT January 1998 DOD Year 2000 Management Plan. We have modified our management plan based on the updates listed in the DOD Y2K Management Plan. To facilitate USSOCOM Y2K problem resolution and conform to the Office of the Secretary of Defense (OSD) mandates, all of the management phases and associated tasks are being executed in accordance with (IAW) the DOD Management Plan.

RECOMMENDATION 2: Continue to identify mission critical systems that USSOCOM manages.

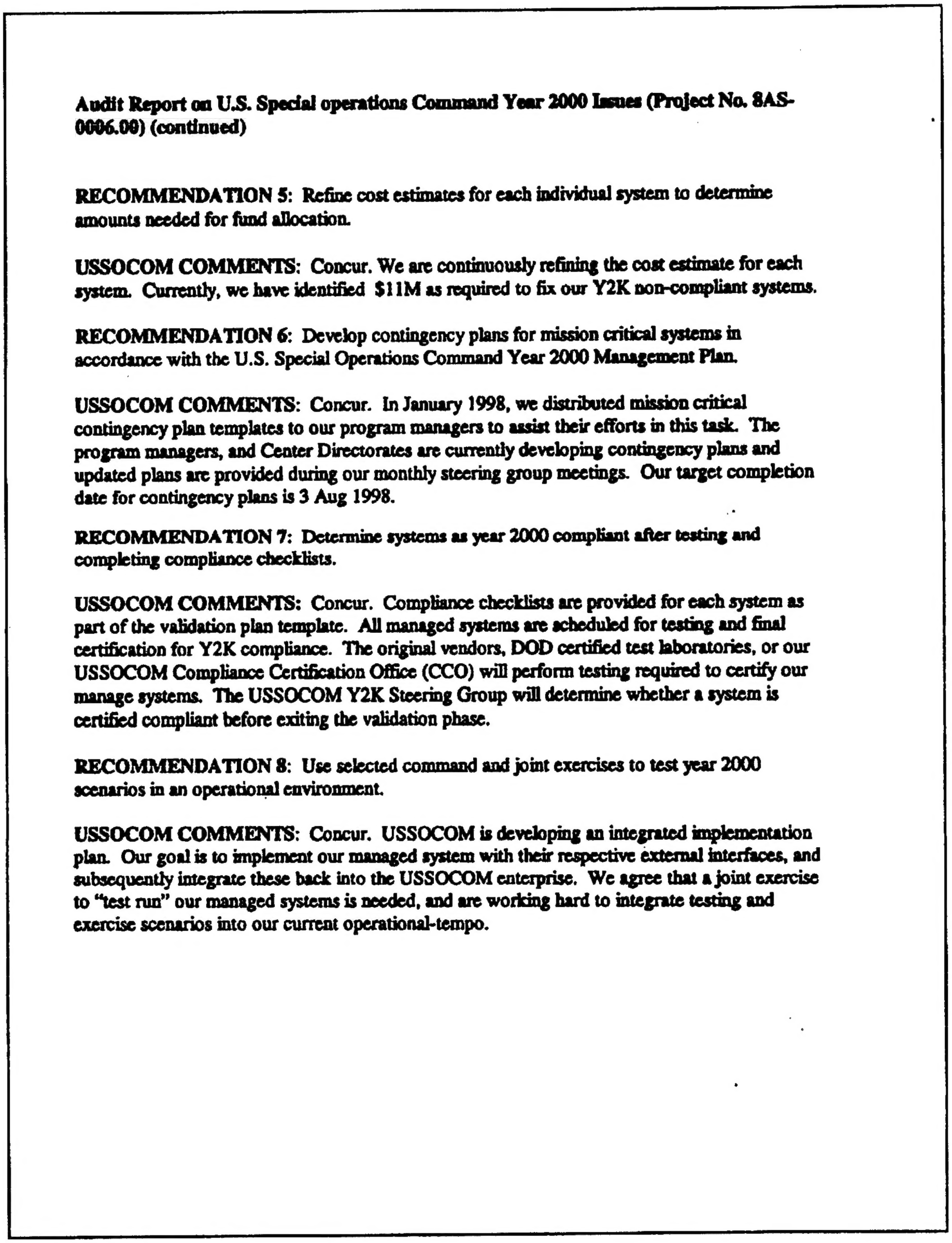
USSOCOM COMMENTS: Concur. Our Y2K program management personnel identified 37 USSOCOM managed mission critical systems as of Feb 23, 1998. The USSOCOM Y2K Steering Group evaluated our mission-critical systems and ranked them in priority order based on their criticality. These mission critical systems were reported to the Joint Staff via e-mail in March 1998. We will record this data into the Defense Integrated Support Tool (DIST) when the DIST system becomes operational. We will provide an updated USSOCOM managed mission critical systems status in the upcoming April 1998 Y2K Quarterly Report.

RECOMMENDATION 3: Continue to identify interfaces and prepare written interface agreements for mission critical systems that USSOCOM manages.

USSOCOM COMMENTS: Concur. This is an on-going effort. As of March 1998, we identified 141 interfaces between USSOCOM managed systems and the supporting systems that are managed by Services or other organizations. Currently, we are developing memorandums of agreement (MOAs) for our external interfaces. The target completion date for all interface MOAs is 3 August 1998. We will provide an interface update in our April 1998 Y2K Quarterly Report.

RECOMMENDATION 4: Continue to identify mission critical supporting systems that Services or other organizations manage.

USSOCOM COMMENTS: Concur. To date, we have identified 68 mission critical supporting systems. As an ongoing effort, USSOCOM will continue to identify mission critical supporting systems. In January 1998, we submitted a list of our mission critical supporting systems to the Joint Staff to distribute to the services and other organizations. We will report our mission critical supporting systems to the Joint Staff in the April 1998 Y2K Quarterly Report.



Audit Report on U.S. Special operations Command Year 2000 Issues (Project No. 8AS-0006.00) (continued)

RECOMMENDATION 5: Refine cost estimates for each individual system to determine amounts needed for fund allocation.

USSOCOM COMMENTS: Concur. We are continuously refining the cost estimate for each system. Currently, we have identified $11M as required to fix our Y2K non-compliant systems.

RECOMMENDATION 6: Develop contingency plans for mission critical systems in accordance with the U.S. Special Operations Command Year 2000 Management Plan.

USSOCOM COMMENTS: Concur. In January 1998, we distributed mission critical contingency plan templates to our program managers to assist their efforts in this task. The program managers, and Center Directorates are currently developing contingency plans and updated plans are provided during our monthly steering group meetings. Our target completion date for contingency plans is 3 Aug 1998.

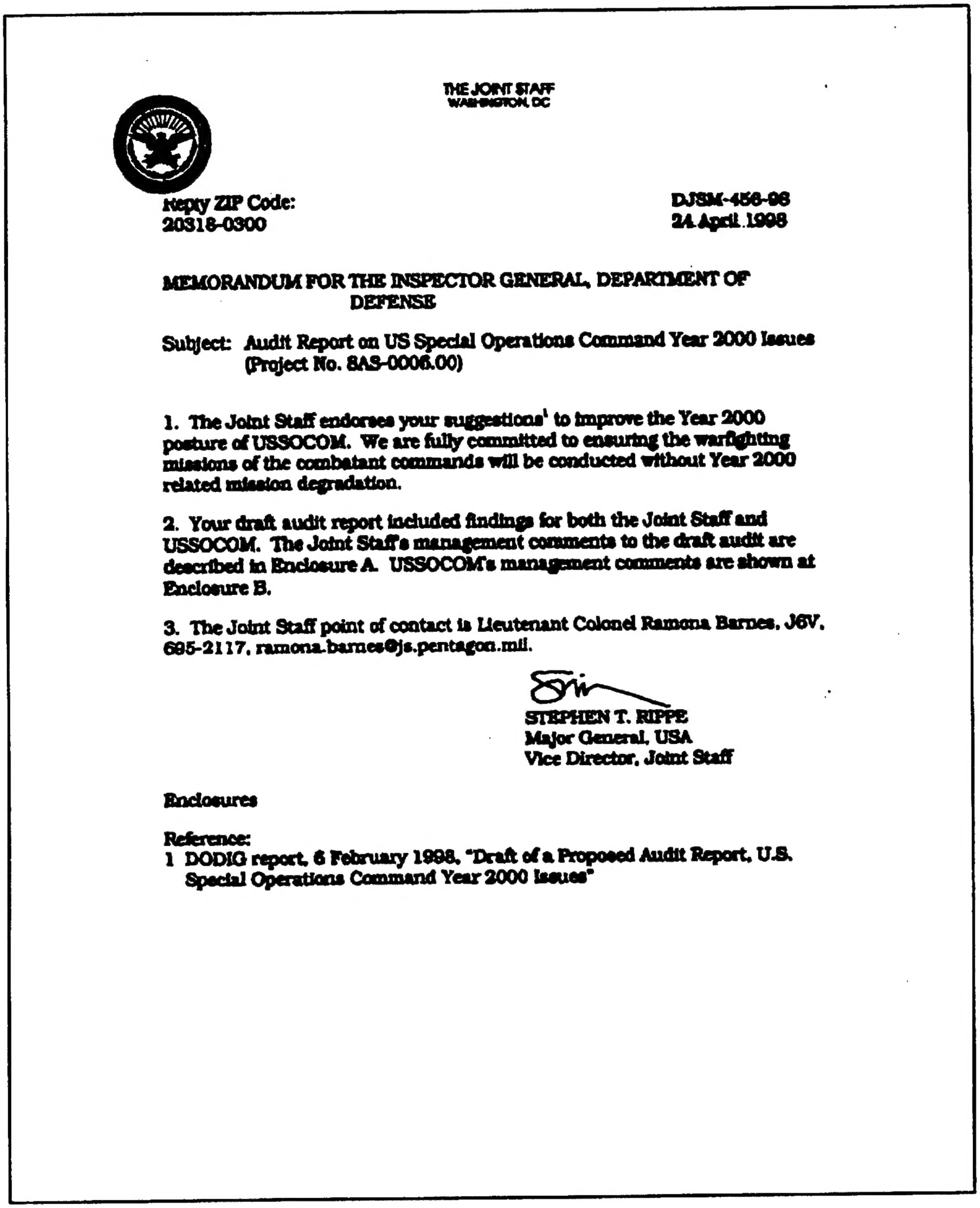
RECOMMENDATION 7: Determine systems as year 2000 compliant after testing and completing compliance checklists.

USSOCOM COMMENTS: Concur. Compliance checklists are provided for each system as part of the validation plan template. All managed systems are scheduled for testing and final certification for Y2K compliance. The original vendors, DOD certified test laboratories, or our USSOCOM Compliance Certification Office (CCO) will perform testing required to certify our manage systems. The USSOCOM Y2K Steering Group will determine whether a system is certified compliant before exiting the validation phase.

RECOMMENDATION 8: Use selected command and joint exercises to test year 2000 scenarios in an operational environment.

USSOCOM COMMENTS: Concur. USSOCOM is developing an integrated implementation plan. Our goal is to implement our managed system with their respective external interfaces, and subsequently integrate these back into the USSOCOM enterprise. We agree that a joint exercise to "test run" our managed systems is needed, and are working hard to integrate testing and exercise scenarios into our current operational-tempo.

Joint Staff Comments



THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM-456-98
24 April 1998

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Subject: Audit Report on US Special Operations Command Year 2000 Issues (Project No. 8AS-0006.00)

1. The Joint Staff endorses your suggestions[1] to improve the Year 2000 posture of USSOCOM. We are fully committed to ensuring the warfighting missions of the combatant commands will be conducted without Year 2000 related mission degradation.

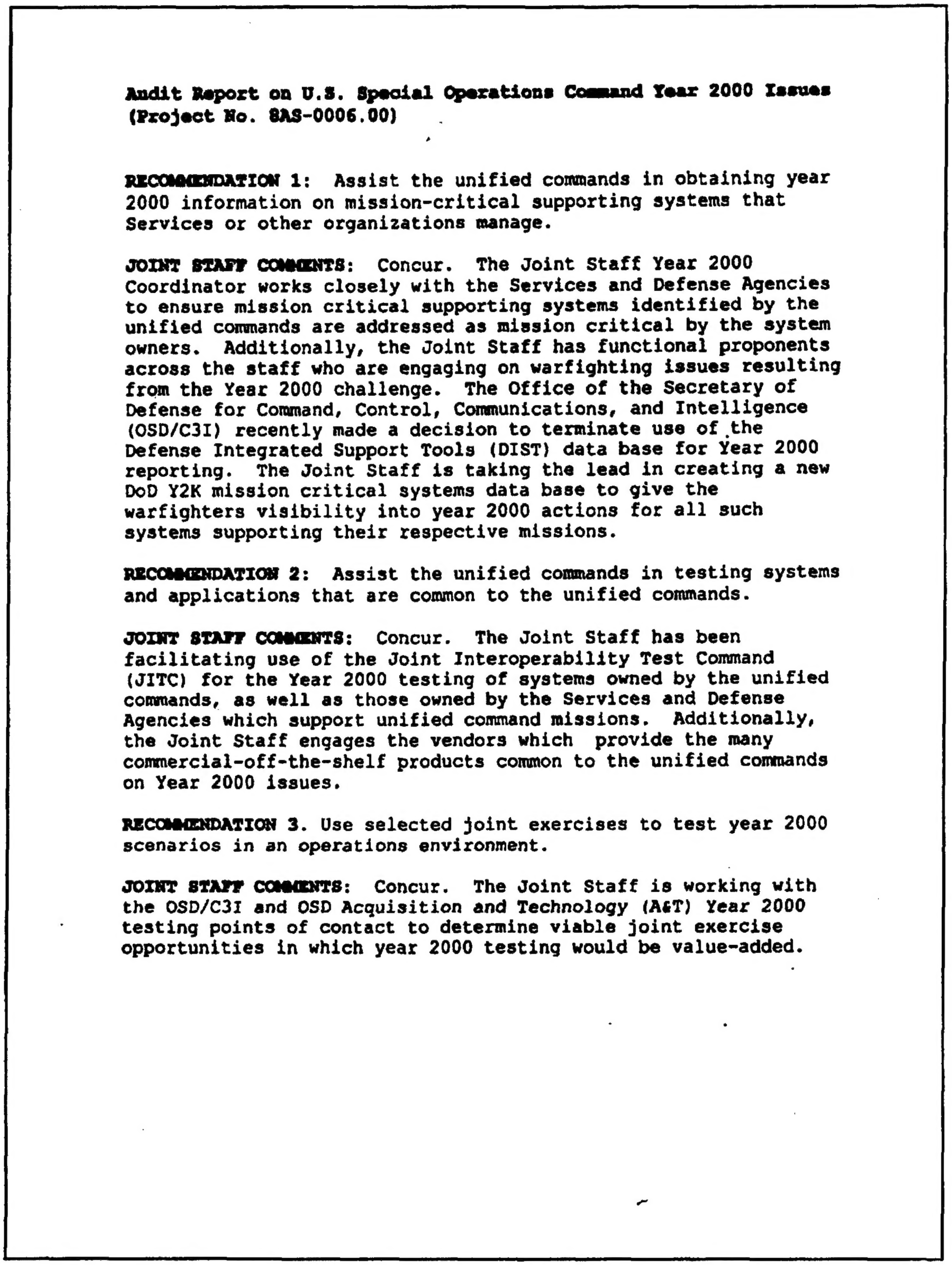
2. Your draft audit report included findings for both the Joint Staff and USSOCOM. The Joint Staff's management comments to the draft audit are described in Enclosure A. USSOCOM's management comments are shown at Enclosure B.

3. The Joint Staff point of contact is Lieutenant Colonel Ramona Barnes, J6V, 695-2117, ramona.barnes@js.pentagon.mil.

STEPHEN T. RIPPE
Major General, USA
Vice Director, Joint Staff

Enclosures

Reference:
1 DODIG report, 6 February 1998, "Draft of a Proposed Audit Report, U.S. Special Operations Command Year 2000 Issues"



Audit Report on U.S. Special Operations Command Year 2000 Issues (Project No. 8AS-0006.00)

RECOMMENDATION 1: Assist the unified commands in obtaining year 2000 information on mission-critical supporting systems that Services or other organizations manage.

JOINT STAFF COMMENTS: Concur. The Joint Staff Year 2000 Coordinator works closely with the Services and Defense Agencies to ensure mission critical supporting systems identified by the unified commands are addressed as mission critical by the system owners. Additionally, the Joint Staff has functional proponents across the staff who are engaging on warfighting issues resulting from the Year 2000 challenge. The Office of the Secretary of Defense for Command, Control, Communications, and Intelligence (OSD/C3I) recently made a decision to terminate use of the Defense Integrated Support Tools (DIST) data base for Year 2000 reporting. The Joint Staff is taking the lead in creating a new DoD Y2K mission critical systems data base to give the warfighters visibility into year 2000 actions for all such systems supporting their respective missions.

RECOMMENDATION 2: Assist the unified commands in testing systems and applications that are common to the unified commands.

JOINT STAFF COMMENTS: Concur. The Joint Staff has been facilitating use of the Joint Interoperability Test Command (JITC) for the Year 2000 testing of systems owned by the unified commands, as well as those owned by the Services and Defense Agencies which support unified command missions. Additionally, the Joint Staff engages the vendors which provide the many commercial-off-the-shelf products common to the unified commands on Year 2000 issues.

RECOMMENDATION 3. Use selected joint exercises to test year 2000 scenarios in an operations environment.

JOINT STAFF COMMENTS: Concur. The Joint Staff is working with the OSD/C3I and OSD Acquisition and Technology (A&T) Year 2000 testing points of contact to determine viable joint exercise opportunities in which year 2000 testing would be value-added.

Audit Team Members

This report was prepared by the Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Thomas F. Gimble
Patricia A. Brannin
Mary Lu Ugone
Dianna J. Pearson
Hugh G. Cherry
Richard B. Vasquez
Scott S. Brittingham
Jennifer L. Zucal
Cristina Maria H. Giusti